MANAGING FRAUD RISK:
FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

Within the three-lines-of-defence framework, the allocation of fraud risk is often unclear. The first line of defence takes care of the most obvious risks as a part of business-as-usual processes (e.g., first-party fraud in the consumer finance business); however, personnel in these roles generally feel less concerned with the unknown or more exotic fraud risks. Conversely, the audit function approaches fraud risk from a more generic perspective and incorporates it into the overall risk assessment. Auditors focus on the major risks threatening the existence of the organisation. This subdivision of the focus on fraud risk is seldom formally discussed and written down. Consequently, blank spots might persist, and an overlap in responsibilities might lead to inadequate action. This presentation proposes an allocation of the different steps in a fraud risk management framework (prevention and detection, reaction, remediation) to the three lines of defence to ensure full coverage.

PATRICK RISCH, CFE, CIA, CCSA
Fraud Protection Manager
BNP Paribas Fortis
Brussels, Belgium

Patrick has more than 20 years of experience in the financial services sector, mainly focused on internal auditing and fraud risk management. In his current position, he heads the fraud protection department within BNP Paribas Fortis and is responsible for setting up and implementing a framework for fraud prevention (policy setting, raising awareness, giving advice, reporting on fraud risk exposure) and fraud detection. Patrick is a master in science and holds certifications in internal auditing, forensic auditing and control self-assessment. He is a board member of the Belgian Chapter of ACFE.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
**MANAGING FRAUD RISK: FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?**

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Purpose of the Presentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>When it comes to managing fraud risk, the “who-does-what” question and—more important—the “who-is-responsible” questions regularly arise.</td>
<td></td>
</tr>
</tbody>
</table>

In general, a territory battle occurs when different executives want to annex another area of competence in order to enlarge their impact. Consequently, the major risk is that different, possibly contradictory, directives are issued.

On the subject of fraud … there are no winners and no prizes at the finish line. And the major risk is that no one really cares.

The purpose of this presentation is to draft a framework to allocate roles and responsibilities in a proactive approach to the management of fraud risk, encompassing prevention, detection, fraud case management, and fraud repair.

**BNP Paribas Fortis**  
BNP Paribas Fortis is the first bank in Belgium to offer a comprehensive package of financial services to private and professional clients, wealthy individuals, corporate clients, public entities and financial institutions through a multi-channel network.  
In Belgium, more than 17,000 staff members service 3.6 million retail customers and 35,000 corporate clients.

Since 2009, BNP Paribas Fortis has been part of the BNP Paribas Group.
MANAGING FRAUD RISK:
FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

Fraud Risk Framework

Why Do People Commit Fraud?

The question of why people commit wrongful acts is as old as the old scriptures. And if we are honest with ourselves, most of us will have to admit that we can imagine a situation in which we would commit such an act. It is a folk wisdom that everyone has his price, although the sum of this price may differ.

Folk wisdowms often are caricatured and simplified representations of reality; nevertheless, let us go a bit further that way. “Bad to the bone” is one aphorism; and “too good for this world” is somehow the opposite.

Translated to the reality of an average population, this means that you have some people who are always looking for an opportunity, without any consideration for others, rules, ethics and so on. Some people are dishonest all of the time. Conversely, you have people who will obey the rules up to the point where it becomes absurd. The red traffic light in the desert that remains red for half a day, the typical whistleblowers. Some people are honest all of the time.

These two groups of people are extremes on a continuum, where most people are honest some of the time and some people are honest most of the time. People let their behaviour largely depend on what is happening around them: what are the others doing; are there controls in place; how does the “authority” react; how badly do I need the money?

Both extremes probably understand each other, and probably have big difficulty in understanding the large

______________________________
1 Quotes from Tommie Singleton, Ph.D., University of Alabama
category that separates them, because people in the middle ground can so easily be influenced.

Unfortunately, we cannot exclusively hire “good people.” Not only is it difficult to distinguish them, but there are probably too few of them to give every employer a chance. However, when we look at this from a perspective of fighting fraud, it can lead us to a few useful considerations:

- We have to avoid hiring “bad people.” This might seem obvious, but the importance of the fact increases when we take into account the impact that personnel has on business. This means that thorough pre-employment screenings are important. Calling a previous employer is not a luxury. It is obvious that we will not succeed in avoiding all miscreants—after all, they are masters in deception—but it is clear that every villain we keep outside is a gain for our organisation.

- Even though “good people” seem to flourish in risk and control departments, we may not isolate them in that environment. When they are spread throughout the organisation, they can influence the situational people around them.

- And finally, the situational people need, above all, a well-developed control environment, with an organisational culture that is imbued by the need for integrity and with an example-setting management style.

In order to set up this healthy control environment, it is important to bear in mind the three drivers that cause someone to commit a fraud, the elements of our well known fraud triangle:
MANAGING FRAUD RISK:
FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

- Opportunity: a sound internal control system helps reduce the risk of errors and subsequently the risk of fraud.
- Pressure: balanced target setting helps to reduce the risk of unwanted activities focused on achieving impossible targets.
- Rationalisation: an organisational culture that cherishes integrity, compliance, and team spirit increases the threshold to colour outside the lines.

**Steps in Fraud Risk Management**
We’ve just learned that in nearly every organisation we will have people who are tempted to defraud us at some moment in their career. Whether we like it or not, this makes it necessary to manage the operational risk called *fraud*. Of course, any comparison is lame, but I like to compare the management of this fraud risk with health care.

The first step is prevention. From all perspectives, this is the best approach: in general, it is the cheapest way, for you as well as for society, and you don’t get actually sick.

However, you have to be aware that most of it you have to do yourself: don’t smoke, don’t drink too much, have some exercise … in a few words, a healthy lifestyle. Health care professionals can help you do this, for example during a regular check-up, but it remains your responsibility.

When you do get ill, you are glad that you can ask a specialist to look after and take care of you. He will do what he can to help you, but this will cost you more, it will take a lot of your valuable time and might even leave you with some scars.
Managing Fraud Risk: First, Second or Third Line of Defence Responsibility?

Afterward, a physiotherapist helps you to revalidate and to take up your life. In case things don’t turn out well, an autopsy can show what went wrong, and this knowledge can help others avoid getting in the same painful situation.

Likewise, in fraud risk management, prevention is the best, and the cheapest way. But, here as well, the management has to take up their responsibility to ensure that the entity remains healthy. Of course, fraud professionals can be of a great help, but it remains the responsibility of the management to take action: assessing the risk, putting controls in place, making sure the organisation is well armed against fraud risk.

When an alleged fraud incident takes place, a professional inquiry will have to reveal what actually happened, to determine the losses and responsibilities, and to decide upon guilt and innocence. This inquiry will most probably have to be carried out within a very strict regulatory or legal framework. This requires skills and competences we do not expect from an average manager, and consequently is it more appropriate to dedicate this responsibility to a specialised team.

Once the fraud scheme has been unravelled, it is again the responsibility of management to book the appropriate accounting corrections, to take disciplinary actions when appropriate and to enhance the system of internal control to avoid reoccurrence. Fraud specialists can also help management to see clearly to the root causes.
### Fraud Risk Management: Putting It into Practice

#### Prevention

**POLICY**

In any organisation of considerable size, and in particular in a highly regulated sector like the financial services sector, you can find formal policies on almost everything, from gifts and entertainment to personal transactions. So, why take the effort to write down yet another policy?

The consequences of a fraud incident can be enormous, both financially and with respect to the reputation of the organisation. Besides this, we’ve explained before that the majority of staff can and will be influenced by the environment. A formal statement by the highest executives in the organisation to this respect has an impact, provided—of course—that these nice words are not contradicted by the behaviour at the top.

In fact, there is only one thing worse than not having a clear anti-fraud statement from the highest authority in the organisation, and that is having a beautiful statement overruled by any person with authority. When it comes to adopting bad habits, most people learn very quickly.

An anti-fraud policy should clearly define:
- What is considered fraud in the organisation
- How the governing bodies of the organisation expect management and staff to deal with fraud risk
- Who is responsible for managing fraud risk
- What to do in case of a fraud suspicion
- What the consequences of fraudulent behaviour are
LEARNING TO TALK ABOUT FRAUD

When management is convinced of the importance of fraud risk management, and when it has been established in an anti-fraud policy, the next step is to spread the message throughout the organisation. After all, staff members at every level will have to recognise fraud in their daily operations, to consider fraud risk when developing processes, and to detect fraud when performing controls. Management at all levels will have to take this into account when planning and controlling.

In the first place, this means that fraud risk should be included in all regular management and product trainings. It makes no sense to talk about how to sell a financial product and not to mention the risks that are related with it. Just dealing with those risks in a separate training program stresses the perception that risk management is “something aside.”

Nevertheless, it is worthwhile to give from time to time training on fraud risk, for example, to illustrate for new comers the specific aspects and to show that fraud schemes (e.g., identity theft), can take different shapes depending on the precise approach of the fraudster. And in particular it is important to give a dedicated training to new managers. Indeed, their role is essential, in building up a control environment and in working out the control activities.

Fraud is often a difficult issue to talk about and people at all levels in the organisation look for excuses. In fact, it is typically one of those topics that you try to hide by just not talking about it. Perhaps another link with healthcare …
And actually, there is some truth in it: if you don’t talk about fraud, you won’t look for fraud, and you will have less fraud in your accounting books. Unless a third party—a customer or a supplier—has been harmed, you probably never will find out. The fraudulent loans are booked along with the bad loans, and simply increase your bad debt ratio. If travel expenses increase, we will just ask for a bigger budget next year.

In the end, this is why it is so important to talk about fraud: to know the real cost of it, and to be able to take appropriate action.

It is only by demonstrating the real cost of fraud that you can convince the target-oriented business managers of what is in it for them: How many loans do they have to sell in order to win back the losses of one fraudulent loan? This means that, by protecting themselves against fraudsters, in fact they are working on their business targets.

Convincing people of the importance of talking about fraud is one thing, giving them the means and tools to do so is another. Therefore we have designed a fraud risk framework with business-specific fraud risk categories, based on the well-known fraud tree.

**ASSESSING FRAUD RISK**
The next step is to think about how fraud risk can materialise in the daily environment of the organisation and how this risk can be mitigated.

In general, when the average manager is asked to think about fraud risk in his entity, he focuses on...
the incidents he has encountered personally, or that are well known for his business, and on incidents that had a great exposure in the media. A fraud risk assessment can help the manager get a complete overview of the risk exposure of his entity, and to assess whether the residual risk is within its tolerance.

A nice side effect of such an exercise is that it puts fraud on the agenda; it forces the manager to think about fraud with an open mind, at least during the two hours of the meeting. In fact, I’m fairly sure that it lasts longer than that.

To make sure that this fraud risk assessment exercise encompasses the whole spectrum of possible fraud risks, we have developed the following methodology.

**PRELIMINARY QUESTIONNAIRE**

In a first stage, a preliminary questionnaire is sent to the interviewee. This questionnaire is composed of about 40 Yes/No questions on 8 topics covering the entire fraud universe.

The purpose is to get an overall starting point regarding some basic issues, for example, is there any cash on hand in the entity? The underlying thought is clearly that, if there is cash on hand, it can be embezzled.

The answers to these questions are not an assessment on their own, but are guidance for the assessor, allowing him to leave some obviously risk-free areas aside, and to challenge the interviewee whenever needed.
Indeed, each of these questions is related to one or more fraud risk categories in our framework, to be discussed in the next phase of the assessment.

**ACTUAL ASSESSMENT**

In the actual fraud risk assessment, a number of typical fraud scenarios (or questions about those scenarios) are presented to the interviewee.

These scenarios cover all fraud risk categories of our framework and use a consistent wording. The interviewee is asked to score a level of concern for both the fraud sensitivity (inherent risk) and the residual risk.

Even though the effectiveness of the controls in place is not actually assessed, we feel that it is from a psychological point of view necessary to give the interviewee the opportunity to express himself in order to get an “honest” opinion on the inherent risk.

**Detection**

When talking about fraud detection, the comparison with the needle in the haystack is often used. Indeed, finding the one fraudulent transfer in almost half a billion genuine transfers, or the one fraudulent physical coupon payment in more than half a million genuine ones is not the easiest task.

To make this mammoth task a bit more manageable, it is useful to take some distance and think about what we are actually looking for.

First of all, in any population of transactions, you will find anomalies and errors. These do not necessarily
### MANAGING FRAUD RISK:

**FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?**

| indicate fraud, but they do point out weaknesses that can lead to fraud. Each one of these weaknesses or anomalies in itself is not really an issue, but a combination thereof is worth investigating. |

| Next we think about which combination of these anomalies or weaknesses might represent in our systems a specific fraud scheme. A mortgage fraud, for instance, is often characterised by an increase of new customers in a branch, living at a considerable distance, asking for a mortgage loan for a renovation. Consequently, we isolate branches with these characteristics, and investigate more in detail the mortgage files. |

| Different fraud schemes thus give rise to different sets of risk factors, allowing a much focused investigation of risky transactions. |

#### Fraud Case Management

Unfortunately, fraud incidents do happen, and require a close examination in order to circumscribe precisely the losses, to find out what exactly went wrong. Regardless of the whether the fraud incident is internal or external, this inquiry has to be carried out in an independent and objective way.

- In a case of an internal fraud, the fraudster or an accomplice might try to destroy or falsify evidence, or management might try to cover up its responsibility in not discovering the fraud earlier.
- External fraud cases are often facilitated by a disrespect of procedures. Subsequently, staff members or managers could be tempted to conceal their mistakes, thus hindering the learning process that should follow any incident.
## MANAGING FRAUD RISK: FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

### Repair and Remediation

Finally, at the end of the story, the mess has to be cleaned up.

- In the first place, the people responsible for the fraud have to be held accountable. This may imply legal and/or disciplinary actions against the fraudster and people who by negligence facilitated the incident.
- Accounting entries are probably necessary to calculate the losses or to rectify fraudulent transactions. It is important that fraud losses are actually registered as such; too often credit losses resulting from a loan fraud are registered as bad loans.
- In case customer assets are stolen, they will have to be reinstated.
- In many cases, it is useful to send out a press release, or at least to have it ready.
- In case there are actually losses, it will be necessary to evaluate whether and how the assets can be recovered.

### Ownership of Fraud Risk

*When It Comes to Fraud, There Are No Winners …*

In general, two contradictory opinions steer the discussion about who owns fraud risk and subsequently bears the final responsibility to manage this risk.

The internal control theory places the responsibility with management at the different levels of the organisation and with all staff members. Setting up a dedicated department will only lull regular management to sleep, leaving them in their comfort zone with the knowledge that fraud risk is being taken care of.
However, specialists might claim that fraud is a very specific risk, and that you cannot expect your average manager or employee to understand the risk well enough to investigate fraud suspicions, to assess the risk, and to work out the necessary preventive and detective controls.

Because of these specificities, depending on the organisation, the responsibility for managing fraud risk can be at different locations and levels or can be allocated to different departments, such as auditing, compliance, safety, and human resources. Sometimes this is a well-thought-out decision but other times it is “because it has always been that way.”

**Three Lines of Defence**

With respect to risk governance within organisations, the three-lines-of-defence model has been increasingly applied over recent years.

In brief, it can be illustrated as follows:²

- As a first line of defence, the organisation’s operational management has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks.
- As a second line of defence, the risk management function (and also other supporting functions like compliance and quality) facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk-related information up and down the organisation.
- As a third line of defence, the internal auditing function will, through a risk-based approach,

---

² Source: [www.eciia.eu](http://www.eciia.eu)
MANAGING FRAUD RISK:
FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

provide assurance to the organisation’s board and senior management, on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate.

To ensure proper management of fraud risk and to maintain coherence with other risk management processes, alignment of the different components of fraud risk with the three lines of defence is required.

**First Line of Defence**

It is obvious that the first responsibility to manage fraud risk lies with the management of the operational entities. After all, they know best the processes and their weaknesses, the products and their risks, and customers and staff members and their particularities, and are the first to react.

Therefore, it is their responsibility to ensure that:

- Staff members receive proper training to recognise fraud and react properly.
- Adequate preventive and detective control measures are in place and functioning.
- Fraud incidents are identified and investigated.
- Lessons are learned from the incident and, if necessary, disciplinary or legal actions are taken.

Of course, we cannot expect every manager in the organisation know how to deal with these issues, in particular the investigation.

It is a good practice to have an employee formally designated by the management team as the anti-fraud expert. The main responsibilities of this person are to keep the story of fraud protection alive in the entity, to
MANAGING FRAUD RISK: FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

maintain the contacts with counterparts in other departments and possibly within other organisations, and to ensure that proper consequence management is in place.

From a theoretical point of view, the management of fraud is a part of mitigating the risk, and thus primarily a responsibility of the management of the operational departments. Or perhaps not … because somehow this issue is a sensitive one.

Nevertheless, only when staff members on the first line of defence take up this responsibility, they will be concerned and driven to mitigate the risk. From a practical point of view, management might consider creating a dedicated competence centre, in particular to fulfil the need for specialised resources or for confidentiality.

It is obvious that, when the incident had—or could have had—serious financial or reputational consequences, the second and third lines of defence will want to have their say. Nevertheless, they should refrain from intervening in the first line of defence’s processes; if they interfere they could compromise their independent view on the fraud-mitigating activities. So they should approach the incidents from their own perspective (i.e., to maintain oversight of the risk control activities and to give assurance to the highest governing bodies of the organisation).

Second Line of Defence
It is the responsibility of the second line to ensure an adequate and consistent approach to fraud risk throughout the organisation, to maintain oversight, and

NOTES
MANAGING FRAUD RISK:
FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?

to report risk and the state of the organisation’s defence system.

In the first place, this will be done by setting the policy and by communicating and enforcing it throughout the organisation. Besides that, there should be regular contacts with management to guide them and assist them in setting up the framework.

Likewise, fraud detection controls can be developed and tested until maturity. After that, they should be transferred to the control framework of the first line.

To summarise, the purpose is not to take over responsibility from line management with respect to fraud risk, but to support management in setting up an adequate fraud prevention and protection framework.

Depending on the size of the organisation and of the fraud risk exposure, this second line can be a part of the risk department or a dedicated, separate department. However, in either case, visibility in the organisation is important.

**Third Line of Defence**
The role of the internal audit department in the management of fraud risk should be limited to providing assurance that the first and second lines are functioning properly and that a specific incident has adequately been addressed.

In this view, the internal audit should avoid starting its own inquiry, apart from ensuring that the first line has dealt with the issue adequately, which is in line with the International Standards for the Professional Practice of Internal Auditing (IIA).
**MANAGING FRAUD RISK: FIRST, SECOND OR THIRD LINE OF DEFENCE RESPONSIBILITY?**

**Shared Responsibilities**

Even though these principles are clear, it is not always easy to determine the concrete responsibilities within this framework, taking into account all players and their respective core tasks.

Without being exhaustive, I have included in the following table the main activities related to the management of fraud risk.

<table>
<thead>
<tr>
<th>1st Line</th>
<th>Prevention and Early Detection</th>
<th>Case Management</th>
<th>Repair and Remediation</th>
</tr>
</thead>
</table>
| • Install a culture of fraud risk awareness.  
• Provide fraud awareness training to staff.  
• Include fraud risk in the overall risk assessment process.  
• Incorporate fraud prevention and detection controls in the operating procedures; segregate duties, monitor adherence to policies and procedures. | • Ensure that a fraud alert hotline is installed and known to everyone in the organisation.  
• Set up a process for the management of fraud cases.  
• Investigate all fraud cases in a professional and objective way. | • Make the necessary accounting entries and register losses.  
• Reimburse customers.  
• Take disciplinary action toward the perpetrator.  
• Improve internal control. |
| 2nd Line | • Oversee fraud risk management activities within the organisation.  
• Give guidance, advice, and recommendations to line management.  
• Maintain fraud risk assessment methodology and oversight on roll out.  
• Serve as the knowledge centre on fraud risk.  
• Develop fraud detection controls. | • Report on fraud risk exposure. | • Conduct post-mortem analyses and make recommendations to line management.  
• Monitor the evolution of fraud risk exposure. |
| 3rd Line | • Provide assurance to the organisation’s board and senior management that fraud risk is managed in an effective way by the organisation. | | |
**Conclusion**

Fraud risk is too important to ignore. Not only can the losses be significant, but the reputational risk is very important as well, in particular for a financial institution. This brings forward the need for a dedicated to mitigate this risk through the lines of defence of the organisation.

From this perspective, creating the second line of defence with the primary goal of fraud risk management is a good practice. Without taking over any responsibility, this role can give guidance to the organisation’s management with respect to fraud risk and monitor the organisation’s exposure and mitigation activities.

To ascertain a coherent approach throughout the organisation, it is important that one definition and one language are used on all fraud risk activities—when training staff on fraud risk awareness, when assessing fraud risk, and when reporting on fraud risk exposure and losses.

Fraud detection can be a meaningful and detect risky situations early, before a fraud actually occurs or at least before the losses become high. In an average organisation at the beginning of the 21st century, and in particular in a financial services organisation, a lot of data is available in the different systems and data warehouses. A statistical approach can allow you to isolate in this sea of transactions the information that you need to find out who is cheating you.

The combination of these elements forms a complete and proactive approach to mitigate fraud risk. Of course, this does not guarantee a fraud-free organisation. However, it prevents giving fraudsters unnoticed and unrestrained access to your assets.